THE HONORABLE JOHN H. CHUN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

AVELARDO RIVERA and YASMINE ROMERO, individually, and on behalf of all others similarly situated, Plaintiffs, v. AMAZON WEB SERVICES, INC., Defendant.	No. 2:22-cv-00269-JHC AMAZON WEB SERVICES, INC.'S REPLY IN SUPPORT OF RULE 12(b)(6) MOTION TO DISMISS NOTE ON MOTION CALENDAR: November 16, 2022 ORAL ARGUMENT REQUESTED

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

TABLE OF CONTENTS

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

TABLE OF AUTHORITIES

Page(s)

CASES

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

STATUTES

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

INTRODUCTION

As explained in AWS's opening brief (Dkt. 45), Plaintiffs seek to hold AWS liable under the Illinois Biometric Information Privacy Act ("BIPA") merely because ProctorU, an AWS customer, used AWS's cloud-based services to interact with Plaintiffs. No court has ever endorsed such a sweeping interpretation of BIPA, and it has no basis in BIPA's text or purpose. Equally important, adopting Plaintiffs' novel reading of the law would have absurd and disastrous consequences for *all* cloud-based data processing everywhere, not just AWS and not just in Illinois. Nothing in Plaintiffs' opposition brief (Dkt. 48) alters those conclusions. The Court should grant AWS's motion to dismiss.

ARGUMENT

A. AWS Complied with BIPA

To be sure, the parties disagree about whether BIPA applies to back-end service providers like AWS. But even assuming Plaintiffs are right and BIPA does apply to AWS in this context (it does not), Plaintiffs do not dispute that there must be some reasonable way for AWS to comply with the statute. *See* Dkt. 45 at 23. And as multiple courts have recognized, the only reasonable way for companies like AWS to do so is to require their customers to fulfill BIPA's requirements, including BIPA's notice-and-consent requirements.[1] *See id.* AWS did exactly that. *See id.* at 24.

Plaintiffs simply assert that this is insufficient. But why? Plaintiffs do not even try to distinguish the multiple cases holding otherwise. Nor do they cite any authority of their own.[2] Instead, they rely on the supposed procedural defect that the AWS Service Terms "are not properly before the Court." Dkt. 48 at 22. But Plaintiffs dispute neither the Service Terms'

---

[1] Indeed, Plaintiffs' counsel previously agreed that AWS could "craft customer agreements that could satisfy BIPA." *See* Dkt. 27 at 7.

[2] The Court should ignore Plaintiffs' insinuation that ProctorU did not comply with BIPA, particularly since their support for that proposition is their attorneys' *brief* opposing ProctorU's motion to dismiss in *Thakkar v. ProctorU, Inc*. *See* Dkt. 48 at n.6. (citing *Thakkar v. ProctorU, Inc.*, Case No. 2:21-cv-01565-NAD, Dkt. 29 (N.D. Ala. July 7, 2021)).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

authenticity nor their incorporation by reference into the FAC. *See* Dkt. 45 at 8, n.3 (citing *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005)). That argument therefore fails.

As a backstop, Plaintiffs argue half-heartedly that "it is hard to see how requiring compliance with the law generally, rather than the [*sic*] BIPA specifically, truly is sufficient." Dkt. 48 at 22. But BIPA itself includes no such "magic words" requirement, and contracts cannot be drafted to identify with specificity every law and regulation that may be implicated in every jurisdiction. Further, AWS's Service Terms demand *more* than general compliance with the law. They specifically require ProctorU to provide "adequate *privacy* notices" and to "obtain[] necessary consent[s]," including "obtaining any required consent of individuals appearing in any images or videos processed by" Rekognition. Dkt. 46-1, Ex. D ¶ 50.4 (emphasis added). Those specific directives are more than adequate to put a Rekognition customer like ProctorU on notice of its obligations to comply relevant privacy laws, including BIPA. And while Plaintiffs claim that AWS should have gone even further and created an "agency relationship" with ProctorU or "followed up" to monitor ProctorU's BIPA compliance, Dkt. 48 at 22-23, neither BIPA's text nor any case interpreting it imposes any such requirements. Ultimately, the key question is whether ProctorU was "contractual[ly]" required to comply with BIPA when it used AWS's services. *See Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 783 (N.D. Ill. 2020). All agree the answer is "yes." Plaintiffs' claims therefore fail.

B. AWS Did Not "Possess" or "Collect" Plaintiffs' Data

1. Plaintiffs allege no facts showing that AWS "possessed" their data.

To avoid dismissal of their Section 15(a) claim, Plaintiffs must plausibly allege that AWS "possessed" their data. *See* 740 ILCS 14/15(a). That they cannot do. *See* Dkt. 45 at 7-12.

Plaintiffs argue that AWS possessed their data under Section 15(a) because ProctorU stored their data in ProctorU's private S3 buckets on AWS's servers. *See* Dkt. 48 at 7. Plaintiffs are wrong. Under Illinois law, "possession" occurs "when a person has or takes control of the subject property or holds the property at his or her disposal." *People v. Ward*, 830 N.E.2d 556,

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

560 (Ill. 2005) (internal quotation marks omitted). Here, Plaintiffs do not allege that AWS exerted or could have exerted *any* control over the data that ProctorU purportedly stored in its private S3 buckets. Indeed, Plaintiffs do not even allege that AWS knew or had reason to know about any such data. Rather, Plaintiffs' FAC fulsomely describes how AWS customers, including ProctorU, exercise exclusive control over their end users' data. *See, e.g.*, FAC ¶¶ 25-32. And, in a moment of revealing candor, Plaintiffs' opposition brief even describes the data ProctorU stored in its private S3 buckets as ProctorU's "property," Dkt. 48 at 7, further emphasizing ProctorU's exclusive control over the data. *See United States v. Gen. Motors Corp.*, 323 U.S. 373, 377-78 (1945) ("property" means "the right to possess, use and dispose of"). In short, Plaintiffs' own allegations and arguments make clear that only ProctorU exercised control over Plaintiffs' data, and therefore only ProctorU—not AWS—possessed Plaintiffs' data.

At bottom, Plaintiffs' possession argument amounts to this: because they alleged that ProctorU stored Plaintiffs' data on AWS's servers, Plaintiffs have alleged that AWS possessed that data. *See, e.g.*, Dkt. 48 at 7. But as courts interpreting Section 15(a) have made clear, mere *storage* is not the same as *possession*. *See Jacobs v. Hanwha Techwin Am., Inc.*, No. 21 C 866, 2021 WL 3172967, at *3 (N.D. Ill. July 27, 2021); *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) ("*Heard I*"). Plaintiffs try to distinguish *Jacobs* and *Heard I* on the basis that those cases addressed instances where plaintiffs failed to allege *how* and *whether* defendants controlled data, not whether defendants had "*sufficient* control over the information." Dkt. 48 at 6. But that argument is not only confusing, it is incorrect. Each of those courts specifically held that allegations of storage like those made in the FAC do not equate to possession under BIPA. *See Jacobs*, 2021 WL 3172967, at *3 ("[P]laintiff here does not provide any factual allegations that plausibly establish that the defendant exercised control over plaintiff's data or otherwise held plaintiff's data at its disposal."); *Heard I*, 440 F. Supp. 3d at 968 (holding that the plaintiffs' allegation that the defendant "stored" fingerprint data "does not plead that BD exercised any form of control over the data or that it held the data 'at [its]

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

disposal'").[3] This Court should do the same.

2. Plaintiffs allege no facts showing that AWS "collected" their data.

Plaintiffs' Section 15(b) claim fails for similar reasons. To avoid dismissal of that claim, Plaintiffs must adequately allege that AWS "collected" Plaintiffs' data. *See* 740 ILCS 14/15(b).[4] And to allege collection, Plaintiffs must allege that AWS undertook some "affirmative act" or engaged in "active step[s]" to acquire their biometric data. *Heard I*, 440 F. Supp. 3d at 966.

Plaintiffs do not allege that AWS took any "active step[s]" to obtain their biometric data. In fact, Plaintiffs do not even allege that AWS knew that ProctorU solicited Plaintiffs' data—a point that Plaintiffs do not dispute. Instead, at most, Plaintiffs allege that *ProctorU* actively sought and obtained their biometric data. *See, e.g.*, FAC ¶¶ 38-41, 45-48. Plaintiffs' Section 15(b) claim necessarily fails for that reason. *See Jacobs*, 2021 WL 3172967, at *3; *see also Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019).

Nonetheless, Plaintiffs argue that "[i]t is not at all clear" that they must allege AWS actively sought to collect their data. Dkt. 48 at 4. But the one decision on which they rely—*Figueroa v. Kronos, Inc.*, 454 F. Supp. 3d 772 (N.D. Ill. 2020)—is neither controlling nor persuasive.[5] Plus, multiple decisions make clear that Section 15(b) is triggered only by active,

---

[3] Plaintiffs refer in passing to *Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831 (N.D. Ill. 2021) ("*Heard II*"). But the *Heard II* court did not hold that storage amounts to possession. *Cf. Heard I*, 440 F. Supp. 3d at 968. The court allowed Section 15(a) claims to proceed after the plaintiff, unlike the Plaintiffs here, added further allegations suggesting that the defendant exercised control over the data stored on its servers. *See Heard II*, 524 F. Supp. 3d at 840. Plaintiffs also rely on *Naughton v. Amazon.com, Inc.*, No. 20-cv-6485, 2022 WL 19324 (N.D. Ill. Jan. 3, 2022). But there, the plaintiff alleged that *Amazon itself* stored biometric data in a database *wholly controlled by Amazon*. That is not what Plaintiffs allege here. *See supra* at 2-3.

[4] To be precise, Section 15(b) applies to entities that "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data. 740 ILCS 14/15(b). For brevity, AWS uses the word "collect" to encompass all the operative terms. Plaintiffs adopt the same convention.

[5] *Figueroa* sought to elide the textual differences between Section 15(a) (which requires possession) and Section 15(b) (which requires collection) by reading BIPA to mean that "Section 15(a) extends to entities that, prior to BIPA's effective date, already possessed biometric information, while Section 15(b) covers only those entities that came into possession of such information after BIPA's effective date." 454 F. Supp. 3d at 784. To AWS's knowledge, no other court has adopted this novel interpretation, which finds no support in BIPA's text.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

affirmative efforts to collect data. *See, e.g.*, *Naughton*, 2022 WL 19324, at *3; *Heard I*, 440 F. Supp. 3d at 966; *Jacobs*, 2021 WL 3172967 at *2; *Namuwonge*, 418 F. Supp. 3d at 285.

Implicitly conceding that active collection is required, Plaintiffs swiftly abandon their argument to the contrary and contend that they *have* alleged active collection by AWS. In particular, Plaintiffs say that they have alleged that AWS, "using Rekognition, performed facial recognition [on Plaintiffs' images] and stored the extracted data [about Plaintiffs] on its servers." Dkt. 48 at 2; *see also, e.g.*, *id.* at 6, 9-10 (same). That argument fails for two reasons.

First, the argument grossly mischaracterizes the FAC. The FAC does *not* allege that AWS "performed facial recognition" on images and then stored the resulting data on its servers. To the contrary, the FAC clearly and consistently alleges that AWS customers, like ProctorU, must take a series of affirmative steps to use Rekognition in their own products and services. *See, e.g.*, FAC ¶¶ 29-30. The FAC goes on to allege that ProctorU did precisely that, *see id.* ¶ 34, and that ProctorU—not AWS—then obtained Plaintiffs' images, performed facial recognition on them, and stored and processed the resulting data in its private S3 buckets. *See, e.g.*, *id.* ¶¶ 41, 48 (alleging that "ProctorU used Amazon Rekognition to perform facial recognition on" Plaintiffs). In other words, the "precise allegation" in the FAC is that ProctorU "collected [Plaintiffs' biometric data] using a system that [AWS] supplied to" ProctorU. *Namuwonge*, 418 F. Supp. 3d at 286. That allegation is insufficient, and Plaintiffs cannot revise their FAC via their opposition brief. *See, e.g.*, *Schneider v. Cal. Dep't of Corr.*, 151 F.3d 1194, 1197 n.1 (9th Cir. 1998).

Second, Plaintiffs could not cure this deficiency by amending their FAC, yet again, to allege that AWS (as opposed to ProctorU) actively collected their data. As even Plaintiffs acknowledge, AWS makes Rekognition generally available to its customers, who may, in turn, use Rekognition to provide products and services to their end users. *See* FAC ¶ 24 (describing Rekognition as a "cloud-based service that . . . makes it easy for [AWS's] customers . . . to add image and video analysis . . . to their applications, products, and services"). AWS does not interact with those end users, and, indeed, has no way of knowing whether and to what extent its

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

customers use Rekognition to interact with their end users. It therefore makes no sense, linguistically or legally, to say that AWS *actively collects* any data from its customers' end users.

3. Plaintiffs' novel interpretation of BIPA is absurd and unworkable.

Plaintiffs' boundless interpretation of BIPA also suffers from a deeper problem: if accepted, it would produce absurd and unworkable results the Illinois legislature never intended. *See* Dkt. 45 at 10-12, 14-16; *see also Solon v. Midwest Med. Recs. Ass'n*, 925 N.E.2d 1113, 1118 (Ill. 2010) (courts must "presume that the legislature did not intend absurd, inconvenient, or unjust consequences"). Plaintiffs' claims should be dismissed for that reason, as well.

Consider Plaintiffs' Section 15(a) claim. Under Section 15(a), companies in possession of biometric data must publish a retention and deletion policy and comply with that policy, including by permanently deleting biometric data "when the initial purpose for collecting or obtaining" the data "has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a). Plaintiffs argue that AWS must comply with those requirements. But as explained in AWS's opening brief, doing so in this context would be impossible because (1) AWS does not know and has no way of knowing whether its customers upload *biometric data* to their S3 buckets; (2) AWS does not know and has no way of knowing whether its customers upload biometric data from *Illinois residents*; and (3) even if AWS could solve those first two mysteries, it still could not determine when Section 15(a)'s deletion requirements have been triggered with respect to any particular end user or any particular biometric data because AWS has no way of knowing the purpose for which that data was collected, whether that purpose has been satisfied, or the date on which end users last interacted with AWS's customers. *See* Dkt. 45 at 10-12.

Plaintiffs' interpretation of Section 15(b) is equally absurd. Section 15(b) requires companies that collect biometric data to provide notice to, and obtain consent from, Illinois residents before collecting any such data. 740 ILCS 14/15(b). Plaintiffs argue that AWS must comply with those requirements, as well. But how? Again, AWS has no way of knowing whether

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

its customers are collecting data from *Illinois residents*, let alone whether its customers are collecting *biometric data* from Illinois residents. And, putting aside those issues, AWS has no way to communicate directly with its customers' end users, which it would have to do in order to provide the notice and obtain the consent contemplated by Section 15(b). *See* Dkt. 45 at 14-16.

These are not mere complaints about inconvenience, as Plaintiffs suggest. The practical implications of Plaintiffs' position are truly astonishing. To comply with Plaintiffs' reading of BIPA, AWS would have to engineer an impossible—and impossibly intrusive—method for analyzing every item of end user data uploaded to every S3 bucket owned by each of the "[t]housands" of companies that use Rekognition, FAC ¶ 4; somehow determine whether any of that data relates to Illinois end users; somehow evaluate whether any data relating to Illinois end users qualifies as biometric data under BIPA; and then devise a way to reach out to AWS's customers' users in order to comply with BIPA's requirements—all *before* any end user biometric data arrives on AWS's servers. Further, Plaintiffs' brief makes clear they believe the same requirements should apply to *all* cloud-service providers—not just AWS. *See* Dkt. 48 at 8. Plaintiffs do not dispute, and their brief does not address that, under their own interpretation of BIPA, companies that provide email services would be deemed to have "collected," and be "in possession" of, all data attached to their users' email messages or stored in their users' email accounts. And to comply with Plaintiffs' interpretation of BIPA, those email providers would have to scan users' messages for biometric data; identify the people from whom that data was collected, or at least identify their state of residency; and then somehow comply with BIPA's requirements with respect to those end users. Apart from being impossibly burdensome, those results would thoroughly undermine consumers' privacy interests—the very interests Plaintiffs purport to champion.

Fortunately, the law requires none of those absurd and untenable consequences. As one court recently explained in rejecting a similarly misguided interpretation of BIPA, the "Illinois legislature clearly contemplated that BIPA would apply [only] in situations"—unlike this one—

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

"where a business had at least some measure of knowing contact with and awareness of the people subject to biometric data collection." *Zellmer v. Facebook, Inc.*, No. 3:18-cv-01880-JD, 2022 WL 976981, at *4 (N.D. Cal. Mar. 31, 2022). Any other interpretation "would lead to obvious and insoluble problems," contrary to "the Illinois legislature's intent." *Id.* at *4-5. The same reasoning applies here and requires rejection of Plaintiffs' claims.[6]

Plaintiffs' response amounts to little more than misdirection. **First,** they argue that "whether the burdens on Amazon to comply with the law truly are insoluble is not an issue that can be resolved on the face of the complaint." Dkt. 48 at 7. Relatedly, they argue that "[t]here is . . . no evidence that other entities would in fact need to change their practices." *Id*. at 8. But Plaintiffs do not dispute any of the reasons why it would be impossible for AWS and other cloud-service providers to comply with Plaintiffs' reading of BIPA. They therefore concede the point. *See Callan v. Motricity Inc.*, No. C11-1340 TSZ, 2013 WL 195194, at *9 (W.D. Wash. Jan. 17, 2013), *aff'd sub nom. Mosco v. Motricity, Inc.*, 649 F. App'x 526 (9th Cir. 2016). And even if they had not conceded the point, discovery is not needed to show that Plaintiffs' position would impose insuperable burdens on AWS and other providers. Common sense suffices.

Second, Plaintiffs claim their position is supported by case law, specifically, *Vance v. Amazon.com, Inc.*, 525 F. Supp. 3d 1301 (W.D. Wash. 2021) and *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 WL 4164452 (Ill. Cir. Ct. Cook Cnty. Aug. 27, 2021). *See* Dkt. 48 at 7-8. But those cases are very different. In *Vance*, plaintiffs alleged that ***Amazon itself*** "appl[ied] for and download[ed]" a large set of biometric data for its own business purposes. 525 F. Supp. 3d at 1312. Similarly, in *Clearview*, plaintiffs alleged that ***Clearview itself*** collected "publicly-

[6] Plaintiffs try to distinguish *Zellmer* on the ground that the proposed class members in that case were "individuals who had no Facebook account, had not provided their photos to Facebook users for uploading to Facebook, and . . . had not shared their images with a common intermediary." Dkt. 48 at 10. But this case is no different. Here, Plaintiffs and the putative class members do not have AWS accounts and did not provide their images directly to AWS. Nor is it true that "the class members [in this case] have a common relationship through ProctorU." *Id*. In fact, Plaintiffs' proposed class includes not only ProctorU users, but *any* Illinois residents who interacted with *any* AWS customers that used Rekognition. *See* FAC ¶ 52.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

available photos on the Internet" and then extracted biometric data from those images for its own use. 2021 WL 4164452, at *1. Relying on these authorities, Plaintiffs argue that "[i]t is *Amazon* that extracts Plaintiffs['] biometric data using Rekognition." Dkt. 48 at 9-10. But again, this is not what Plaintiffs allege. *Cf.* FAC ¶¶ 41, 48 (alleging that "ProctorU used Amazon Rekognition to perform facial recognition").

Third, Plaintiffs argue that "AWS would not be in violation of its customer agreement by using data within [its customers' S3] buckets to provide notice and obtain consent prior to collecting biometric data in compliance with BIPA."[7] Dkt. 48 at 8-9. That argument misconstrues the AWS Customer Agreement. More importantly, like the "thirteenth chime of a broken clock," it casts doubt on Plaintiffs' entire theory of the case. *Ritchie v. United States*, No. C 00-03940 MHP, 2004 WL 1161171, at *6 (N.D. Cal. May 24, 2004). According to Plaintiffs, AWS could simply use data "within its customers' buckets" to "comply with applicable law," including Section 15(b). Dkt. 48 at 8. But Section 15(b) requires companies to provide notice and obtain consent *before* any biometric data is collected. How, then, could AWS rely on data *already stored* on its servers to provide notice to end users *before* their data is stored on AWS's servers? Here again, the incoherence of Plaintiffs' position is on full display. And even if Plaintiffs' argument were not entirely illogical, by arguing that AWS should use its customers' data to comply with BIPA, Plaintiffs admit and embrace the impossible burdens that their position would impose on cloud-service providers, including the burden of analyzing every item of user content. That simply cannot be squared with the "Illinois Supreme Court's determination that BIPA should not impose extraordinary burdens." *Zellmer*, 2022 WL 976981, at *5.

C. Plaintiffs' Claims Should Be Dismissed Under the Extraterritoriality Doctrine

In addition to the fatal flaws described above, Plaintiffs have not alleged that AWS's

[7] The Court should reject Plaintiffs' half-hearted argument that the Customer Agreement is not properly before the Court, *see* Dkt. 48 at 8, given that the Customer Agreement is incorporated by reference into the FAC. *See supra* at 1. And Plaintiffs' contention that the Customer Agreement is somehow unenforceable is similarly flawed, particularly since the Customer Agreement includes robust notice requirements for any modifications. *See* Dkt. 46-1, Ex. C §§ 2, 12.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

purported misconduct occurred primarily and substantially in Illinois—an essential prerequisite for suing under BIPA. Their claims should be dismissed for that reason, as well. *See* Dkt. 45 at 16-19; *see also McGoveran v. Amazon Web Servs., Inc.*, No. 20-1399-LPS, 2021 WL 4502089, at *3-4 (D. Del. Sept. 30, 2021) (granting motion to dismiss on extraterritoriality grounds).

Plaintiffs' responses are not convincing. **First,** they ask the Court to overlook their failure to allege any Illinois-based conduct because, they argue, whether AWS's misconduct occurred in Illinois is a "highly fact-bound issue." Dkt. 48 at 10-11. But merely because the extraterritoriality issue may call for consideration of "a myriad of factors," as Plaintiffs contend, that does not relieve Plaintiffs of their burden to *plead* facts sufficient to draw the conclusion that some relevant conduct occurred "primarily and substantially" in Illinois. Absent such facts, BIPA does not apply at all. As the Supreme Court has made clear, Plaintiffs may not "unlock the doors of discovery" with "nothing more than conclusions," *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009), or "rely on anticipated discovery" to "fill in the gaps" in their complaint, *Whitaker v. Tesla Motors, Inc*., 985 F.3d 1173, 1177 (9th Cir. 2021). Thus, when a plaintiff fails to allege "any direct interaction with AWS" that "might plausibly be imputed to Illinois"—as is the case here—dismissal is appropriate. *McGoveran*, 2021 WL 4502089, at *5.

Second, as a fallback, Plaintiffs argue that their FAC adequately alleges Illinois-based conduct. Specifically, Plaintiffs argue, their FAC alleges that (1) they reside in Illinois; (2) they uploaded the relevant images from Illinois; (3) they took the relevant exams in Illinois; (4) they allegedly did not receive BIPA-compliant notice from AWS in Illinois; and (5) they suffered their supposed injures in Illinois. Dkt. 48 at 11-12. But in fact, a fair reading of Plaintiffs' FAC reveals no Illinois-based conduct *by AWS*, which is the relevant inquiry under BIPA. *See Vance v. Microsoft Corp.*, No. C20-1082JLR, 2022 WL 9983979, *6-7 (W.D. Wash. Oct. 17, 2022) ("*Vance-Microsoft"*); *Vance v. Amazon.com, Inc*., No. C20-1084JLR, 2022 WL 12306231, *6-7 (W.D. Wash. Oct. 17, 2022) ("*Vance-Amazon*"). Again, Plaintiffs allege that they used ProctorU's services (not AWS's services) to take their exams, and they allege that they uploaded

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

their images to ProctorU (not to AWS). FAC ¶¶ 40-41, 47-48. Further, as the *McGoveran* court explained, merely asserting that AWS failed to provide the requisite notice in Illinois is not enough where, as here, Plaintiffs have "not alleged any activity in Illinois that would impose such obligations on" AWS in the first place. 2021 WL 4502089, at *4.

Third, Plaintiffs claim that the well-reasoned decisions in *Vance-Amazon* and *Vance-Microsoft* are distinguishable because the relevant "images [here] come directly from Illinois." Dkt. 48 at 15. But this is *the same* argument that *Vance-Microsoft* and *Vance-Amazon* reject on the basis that plaintiffs' residency alone is not enough to trigger application of BIPA. *See Vance-Microsoft*, 2022 WL 9983979, at *7; *Vance-Amazon*, 2022 WL 12306231, at *7; *see also McGoveran*, 2021 WL 4502089, at *4. And, more importantly, Plaintiffs do not allege that the relevant images came to AWS "directly" from Illinois; they allege that the images came to AWS via ProctorU (a non-Illinois entity). *See* FAC ¶¶ 40-41, 47-48. BIPA therefore does not apply.

D. BIPA's Financial Institutions Exemption Bars Plaintiffs' Claims

Plaintiffs' claims are also barred because BIPA does not apply "in any manner" to "a financial institution," like the colleges, which are "subject to [the Gramm-Leach-Bliley Act ("GLBA")] and the rules promulgated thereunder." 740 ILCS 14/25(c).

Attempting to rewrite this statutory text, Plaintiffs erroneously argue that the Illinois legislature sought to exempt only "banks" under Section 25(c). Dkt. 48 at 16. But Section 25(c) is not so limited. As "[a]t least five courts have" confirmed, "BIPA section 25(c) applies to institutions of higher education that are significantly engaged in financial activities such as making or administering student loans." *Powell v. DePaul Univ.*, No. 21 C 3001, 2022 WL 16715887, at *3 (N.D. Ill. Nov. 4, 2022) (collecting cases). Judicially noticeable documents properly before the Court show that the colleges are engaged in precisely these activities, on the order of millions of dollars per year. *See* Dkt. 46-1, Exs. G-I; *see also Powell*, 2022 WL 16715887, at *3 (considering similar "publicly available documents"). Thus, even assuming BIPA § 25(c) is an affirmative defense as Plaintiffs contend, Dkt. 48 at 17, the Court may

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

properly resolve it now, given the "materials presented to the court . . . showing [the colleges'] participation in the federal student aid programs are not challenged by" Plaintiffs. *Powell*, 2022 WL 1675887, at *3; *see also Scott v. Kuhlmann*, 746 F.2d 1377, 1378 (9th Cir. 1984) (approving resolving affirmative defenses that "raise[] no disputed issues of fact" at the pleading stage).

Lastly, Plaintiffs argue that Section 25(c) is irrelevant even if the colleges are financial institutions because Section 25(c) only prohibits applying BIPA "directly" to financial institutions. Dkt. 48 at 18-20. But as Plaintiffs admit, *see id*. at 19 n.4, that argument asks the Court to read into Section 25(c) words that are not there. Section 25(c)'s language is simple and clear: it prohibits applying BIPA's requirements to financial institutions "in any manner"—direct, indirect, or otherwise. 740 ILCS 14/25(c). And Plaintiffs' cursory argument that imposing BIPA's requirements on AWS would have no effect on the colleges' remote proctoring activities is mere wishful thinking. Section 25(c) therefore bars Plaintiffs' claims.

E. Plaintiffs Cannot Be "Aggrieved" by AWS's Alleged Violation of Section 15(a)

Lastly, Plaintiffs argue that a person is "aggrieved" under BIPA, and may therefore seek relief under the law, "if their rights under any provision . . . are violated." Dkt. 48 at 22 (citing *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1207 (Ill. 2019)). But to meet that test here, Plaintiffs must show that AWS's alleged failure to publish the retention-and-deletion policy contemplated by Section 15(a) violated their "personal" rights. *Rosenbach*, 129 N.E.3d at 1205 (citation omitted). They cannot make that showing because BIPA does not enshrine a personal right to such a policy; at most, it imposes a duty "to the public generally." *See Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020).[8] Plaintiffs' Section 15(a) claim therefore fails as a matter of law.

CONCLUSION

AWS respectfully requests that the Court grant its Motion to Dismiss (Dkt. 45).

[8] It is true that the Seventh Circuit reached this conclusion in the context of an Article III standing analysis. *See* Dkt. 48 at 21. But Plaintiffs do not argue, nor could they, that the conclusion is irrelevant to the nature and scope of the rights afforded under BIPA.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Dated: November 16, 2022

By: /s/ Ryan Spear

Ryan Spear, WSBA No. 39974
RSpear@perkinscoie.com
Nicola Menaldo, WSBA No. 44459
NMenaldo@perkinscoie.com
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Telephone 206.359.8000
Facsimile 206.359.9000

Attorneys for Defendant
AMAZON WEB SERVICES, INC.